UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/447,500	11/23/1999	ROBERT DAVID GRAHAM	003845.P0001	3902

7590 04/21/2005

EXAMINER	
ARANI, TAGHI T	

ART UNIT	PAPER NUMBER
2131	

W. Scott Petty
KING & SPALDING
191 Peachtree Street
45th Floor
Atlanta, GA 30303-1763

DATE MAILED: 04/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/447,500	GRAHAM, ROBERT DAVID	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 August 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-25 and 32-40* is/are allowed.

6)☒ Claim(s) *26-28 and 31* is/are rejected.

7)☒ Claim(s) *29 and 30* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 July 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-40 have been examined.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.1 14, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.1 14, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.1 14. Applicant's submission filed on 8/25/2004 has been entered.

Drawings

3. The drawings filed on 07/07/204 for figures are acceptable to the examiner .

Response to Amendment

4. Applicant's amendment and remarks filed 07/07/2004 with respect to independent claims 1, 18, and 32 have been fully considered and were found to have allowable subject matter over the prior art of record. Therefor, an examiner's response to the relating arguments is rendered moot. However, the Applicant's arguments relating to the independent claims 26 and 31 have been fully considered but they are not pursuasive.

Applicant's arguments filed 07/07/2004 with respect to analogous art on pages 10 have been fully considered but they are not persuasive.

Claims 26-28 and 31 are rejected under 35 USC 102. The analogous art test (on page 12)

recited by the MPEP 2141 .01(a) is a precaution to the examiner stating that only analogous art can be combined to meet the limitations of a claim for a proper 35 USC 103 rejection. Thus the analogous art argument of the Applicant on page 10 is moot in view of a 35 USC 102 rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. **Claims 26-28 and 31** are rejected under 35 U.S.C. 102(b) as being anticipated by Johnson et al (USP 5,345,595).

As per claim 26, Johnson et al teach:

storing a plurality of suspect-specific alert variables for a plurality of computer network nodes comprising workstations (column 6, lines 61-65);

modifying a network alert variable based on the value of each of said plurality of suspect-specific alert variables (column 9 and column 10, lines 3-44); and

triggering a network response when said network alert variable reaches a predetermined threshold level (column 4, lines 16-26).

As per claim 27, Johnson et al teach notifying each of the plurality of network nodes (system operators) that they should each increase their suspect-specific alert variable (alert-state) towards a particular suspect computer node.

As per claim 28, Johnson et al teach a computer network server node initiating a

passive scan of a particular suspect node (column 24, lines 30- 40). The suspect computer node is monitored (passively) for a window of time.

As per claim 31, Johnson et al teach:

storing a plurality of overall alert variables for a plurality of computer network nodes comprising workstations (column 9, lines 29-43 and column 21, lines 27-50),

modifying a network alert variable based on the value of each of said plurality of overall alert variables (column 9 and column 10, lines 3-44).

triggering a network response when said network alert variable reaches a predetermined threshold level (column 4, lines 24-26 and FIG. 4C block S540).

Allowable Subject Matter

6. Claims 29-30 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claims 1-25, 32-40 are allowed over prior art of record.

Conclusion

7. Prior arts made of record, not relied upon:

US Patent 6,708212 is directed to a method of network surveillance which includes receiving network packets handled by a network entity and building at least one long-term and a least one short-term statistical profile from a measure of the network packets that monitors data transfers, errors, or network connections. A comparison of the statistical profiles is used to determine whether the difference between the statistical profiles indicates suspicious network activity.

US patent 6,453,345 is directed to a network security and surveillance system which passively monitors and records the traffic present on a local area network, wide area network, or other type of computer network, without interrupting or otherwise interfering with the flow of the traffic. Raw data packets present on the network are continuously routed (with optional packet encryption) to a high-capacity data recorder to generate low-level recordings for archival purposes. The raw data packets are also optionally routed to one or more cyclic data recorders to generate temporary records that are used to automatically monitor the traffic in near-real-time. A set of analysis applications and other software routines allows authorized users to interactively analyze the low-level traffic recordings to evaluate network attacks, internal and external security breaches, network problems, and other types of network events.

US Patent 7,725,378 id directed to an active monitor which detects and classifies messages transmitted on a network. In one form, the monitor includes a routine for classifying TCP packet source addresses as being of an acceptable, unacceptable, or suspect type. Suspect source addresses may be further processed in accordance with a state machine having a number of conditionally linked states including a good address state, a new address state, and a bad address state. For this form, the monitor selectively sends signals to targeted destination hosts for addresses in the unacceptable.

US patent 6,301,668 discloses a method and system for adaptive network security using network vulnerability assessment. The method comprises directing a request onto a network. A response to the request is assessed to discover network information. A plurality of analysis tasks are prioritized based upon the network information. The plurality of analysis tasks are to be performed on monitored network data traffic in order to identify attacks upon the network.

US patent 5,991,81 teaches a system and method for network surveillance and detection of attempted intrusions, or intrusions, into the network and into computers connected to the network. The System functions are: (A) intrusion detection monitoring, (B) real-time alert, (C) logging of potential unauthorized activity, and (D) incident progress analysis and reporting. Upon detection of any attempts to intrude, the System will initiate a log of all activity between the computer elements involved and send an alert to a monitoring console. When a log is initiated, the network continues to be monitored by a primary surveillance system. A secondary monitoring process is started which interrogates the activity log in real-time and sends additional alerts reporting the progress of the suspected intruder.

US Patent 5,922,051 teaches a computer network having a plurality of nodes associated therewith, a data traffic management system for managing data traffic among the plurality of nodes, comprising 1) a polling circuit that retrieves node traffic information from the plurality of nodes; and 2) process logic that compares first selected node traffic information associated with a first selected one of the plurality of nodes with a first threshold level to detect a trend in the first selected node traffic information with respect to the first threshold level.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131

4/16/05